Lecture 7.

Def. A subset F_0 of a field F is called a subfield if F_0 is a subring of F and $\forall a \in F_0$, $a \neq 0$ the inverse element a^{-1} lies in F_0.

Example. $\mathbb{Q}$ is a subfield in $\mathbb{R}$, $\mathbb{R}$ is a subfield in $\mathbb{C}$.

If F_0 is a subfield of a field F then F can be viewed as a vector space over F_0.

Now let's come back to a finite field F.

All elements in the infinite sequence

$$\ldots, -1, 0, 1, 2 \cdot 1, 3 \cdot 1, \ldots$$

can not be distinct since F is finite.

Hence F has a positive prime

characteristic p, $\forall a \in F \quad pa = 0$.

Let $F_0 = \{0, 1, 2 1, \ldots, (p-1) 1\}$. Then F_0 is a subfield of F. Why?

The mapping $\varphi : \mathbb{Z}(p) \to F_0$,

$$\varphi : i \bmod p \to i 1$$

is an isomorphism of rings. Being a field is an abstract property. Hence F_0 is a field as well, $F_0 \cong \mathbb{Z}(p)$.

We view F as a vector space over $\mathbb{Z}(p)$.

Let $\dim_{\mathbb{Z}(p)} F = n$. As shown in the previous lecture

$$|F| = p^n.$$

We proved that the order of an arbitrary finite field F is a power of a prime number

(the characteristic of F).

We constructed fields of orders p, 25, 4, 8.

Now our aim is to prove the great theorem of E. Galois:

For every power of a prime number p^n there exists a finite field of order p^n. Moreover, this finite field is unique up to isomorphism.

If we knew that for any prime p and any $d \geq 1$ there exists an irreducible over $\mathbb{Z}(p)$ polynomial $f(t)$ of degree d then we would have a field of order p^d : $\mathbb{Z}(p)[t]/(f(t))$.

But at this point we don't know it.

We will go a different way.

Proposition. Let F be a field, let $f(t) \in F[t]$ be a polynomial of degree ≥ 1. There exists a bigger field $F \subset K$ (here F is a subfield of K) such that $f(t)=0$ has a root in K.

Example. The polynomial t^2+1 does not have a root in $\mathbb{R}$, but it has a root in a bigger field $\mathbb{C}$, $\mathbb{R} \subset \mathbb{C}$.

Proof. Every polynomial $f(t)$ of degree ≥ 1 is a product of irreducible polynomials.

Let $f(t) = P_1(t) P_2(t) \cdots$, the polynomials $P_1(t), P_2(t), \ldots$ are irreducible.

It is sufficient to construct a bigger field $F \subset K$, such that $P_1(t)=0$ has a root in K.

Consider the ideal $(P_1(t))$ in $F[t]$, since

the polynomial $P_1(t)$ is irreducible it follows that the ideal $(P_1(t))$ is maximal, and therefore the factor-ring $F[t]/(P_1(t)) = K$ is a field.

The subset $\{\alpha + (P_1(t)) \mid \alpha \in F\}$ is a subfield of the field K,

$$F \ni \alpha \to \alpha + (P_1(t)) \in K$$

is an isomorphism.

We will identify the field F with the subfield $\{\alpha + (P_1(t)) \mid \alpha \in F\} \subset K$, so

$$F \subset K.$$

The polynomial $P_1(t)$ has a root in K:

$$t + (P_1(t))$$

Indeed, $P_1(t + (P_1(t))) = P_1(t) + (P_1(t)) =$

$(P_1(t)) = 0$ in K. $\square$

Remark. If the field F were countable then the field $K = F[t]/(P_1(t))$ is countable as well.

Def. A field F is called algebraically closed if an arbitrary polynomial $f(t) \in F[t]$ of degree ≥ 1 has a root in F.

The "Fundamental theorem of Algebra": the field $\mathbb{C}$ is algebraically closed.

If K is a field and $F \subset K$ is a subfield of the field K then we call K an extension of F and denote K/F.

Def. An extension K/F is called algebraic if for an arbitrary element $k \in K$ there exists a polynomial $f(t) \in F[t]$ such that

$f(k)=0$.

Lemma. The extension $K=F[t]/(P_1(t))$ of a field F is algebraic.

Proof. Let $\deg P_1(t)=d\geq 1$. We showed above that the factor-ring $F[t]/(P_1(t))$ viewed as a vector space over F is d-dimensional (with a basis $1+(P_1(t)), t+(P_1(t)), \dots, t^{d-1}+(P_1(t))$), $F\subset K$, $\dim_F K=d$.

A fact from Linear Algebra (exercise!): in a d-dimensional vector space any $d+1$ elements $v_1,\dots,v_{d+1}$ are linearly dependent.

Choose an arbitrary element $k\in K$.

~~Conclude~~ Consider $d+1$ elements

$$1, k, k^2, \dots, k^d.$$

There exist coefficients $\alpha_0, \alpha_1, \dots, \alpha_d \in F$, not all equal to 0 such that

$$\alpha_0 1 + \alpha_1 k + \alpha_2 k^2 + \dots + \alpha_d k^d = 0.$$

Consider the polynomial

$$f(t) = \alpha_0 1 + \alpha_1 t + \dots + \alpha_d t^d.$$

then $f(k) = 0$. This proves that the extension K/F is algebraic. $\overline{\nu}$

[see pp. 8.a – 8.f]

Theorem. For an arbitrary field F there exists a field extension L/F such that

1) the field L is algebraically closed,
2) the extension L/F is algebraic.

Proof. We will prove the theorem only in the case when the field F is finite or countable.

Exercise: think how to extend it to a field

An extension of fields

$$F \subset K$$

is called finite if K is finite dimensional as an F-space. The dimension $\dim_F K$ is denoted as $|K:F|$.

We proved above that every finite extension is algebraic.

Lemma. Let K/F be an algebraic extension of fields. For ~~an arbitrary~~ every finite collection of elements $k_1, \dots, k_n \in K$ there exists a subfield K', $F \subseteq K' \subseteq K$ such that $k_1, \dots, k_n \in K'$ and K'/F is a finite extension.

Proof. Let K' be the F-span of all products

$$k_1^{d_1} k_2^{d_2} \cdots k_n^{d_n}, \text{ where } d_1, \dots, d_n \geq 0.$$

Clearly, K' is a subring of K and a vector space over F.

Each element k_i is a root of some polynomial $f_i(t) \in F[t]$. Let

$$f_i(t) = \alpha_{i0} + \alpha_{i1} t + \dots + \alpha_{im_i} t^{m_i}, \quad \alpha_{ij} \in F,$$

so $\deg f_i(t) = m_i$.

It means that $k_i^{m_i}$ is an F-linear combination of $1, k_i, \dots, k_i^{m_i-1}$.

We claim that $\dim_F K' < \infty$. More precisely, K' is spanned by products

$$k_1^{d_1} k_2^{d_2} \dots k_n^{d_n}, \quad 0 \le d_i < m_i, \ i = 1, \dots, n.$$

It means that $\dim_F K' \le m_1 m_2 \dots m_n$.

Indeed, consider a product $k_1^{d_1} k_2^{d_2} \dots k_n^{d_n}$.

Suppose that $d_i \ge m_i$. Then $k_i^{d_i} = k_i^{m_i} \cdot k_i^{d_i - m_i}$.

We replace $k_i^{m_i}$ by a linear combination of smaller powers. Then $k_1^{d_1} k_2^{d_2} \dots k_n^{d_n}$ is replaced by a linear combination of products where the power d_i is smaller. This proves the claim and completes the proof of the lemma.

Remark. We proved that the extension K/F is locally finite.

Lemma. Let $F \subset K \subset L$ be fields. Suppose that the extensions K/F and L/K are finite. Then the extension L/F is finite as well. Moreover, $|L:F| = |K:F| \cdot |L:K|$.

Proof. Let $e_1, \dots, e_n$ be a basis of the F-vector space K. Let $f_1, \dots, f_m$ be a basis of the K-vector space L. Then $\{e_i f_j\}_{\substack{1 \le i \le n \\ 1 \le j \le m}}$ is a basis of the F-vector space L.

Indeed, an arbitrary element $a \in L$ can be represented as $a = \sum_{j=1}^{m} k_j f_j$, $k_j \in K$.

An arbitrary element k_j can be represented as $k_j = \sum_{i=1}^{n} \alpha_{ij} e_i$, $\alpha_{ij} \in F$. Now,

$$a = \sum_{j=1}^{m} k_j f_j = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} \alpha_{ij} e_i \right) f_j =$$

$$= \sum_{i,j} \alpha_{ij} e_i f_j .$$

Hence L is spanned by $e_i f_j$'s over F. It remains to check that ~~e_i~~ $e_i f_j$'s are linearly independent over F. We leave it to you as an exercise. ∎

Lemma. Let $F \subset K \subset L$ be fields. Suppose that the extensions K/F and L/K are algebraic. Then the extension L/F is algebraic as well.

Proof. Choose $a \in L$. Since the element a is algebraic over K it follows that there exist coefficients $k_0, k_1, \dots, k_{m-1} \in K$ such that

$$a^m = k_0 \cdot 1 + k_1 a + \dots + k_{m-1} a^{m-1}.$$

Since the extension K/F is locally finite (see above) there exists a subfield K', $F \subseteq K' \subseteq K$, such that $k_0, k_1, \dots, k_{m-1} \in K'$ and $|K' : F| < \infty$.

Consider the vector space

$$S = K' + K'a + \dots + K'a^{m-1}.$$

It is easy to see that S is a subalgebra of L.

If K' is spanned by elements $e_1, \dots, e_n$ over F, $K' = \sum_{i=1}^{n} F e_i$ then S is spanned by

elements $e_i a^j$, $1 \le i \le n$, $0 \le j \le m-1$.

Hence $\dim_F S < \infty$. Let $\dim_F S = d$.

Then $d+1$ elements $1, a, \dots, a^d$ are linearly dependent over F, that is, there exist coefficients $\alpha_0, \alpha_1, \dots, \alpha_d \in F$, not all $= 0$, such that $\sum_{i=0}^{d} \alpha_i a^i = 0$. Then the polynomial

$$f(t) = \sum_{i=0}^{d} \alpha_i t^i \in F[t]$$ is $\neq 0$ and $f(a) = 0$.

We proved that the extension L/F is algebraic. $\square$

of an arbitrary cardinality.

At first we will construct a field extension K/F such that

1) the field K is finite or countable;
2) every polynomial from $F[t]$ has a root in K;
3) K/F is an algebraic extension.

Since the field F is finite or countable the set of all polynomials over F of degree ≥ 1 is countable. Let us list them all: $f_1(t), f_2(t), \ldots$

there exists a field extension $F \subset K_1$ such that

1) the field K_1 is finite or countable,
2) the polynomial $f_1(t)$ has a root in K_1;
3) the extension K_1/F is algebraic.

The polynomial $f_2(t)$ is a polynomial over F, hence it is a polynomial over K_1. Hence there is a field extension

$$K_1 \subset K_2$$

such that

1) the field K_1 is finite or countable;

2) the polynomial $f_2(t)$ has a root in K_2;

3) the extension K_2/K_1 is algebraic. By the theorem that we proved earlier since K_2/K_1 and K_1/F are algebraic extensions it follows that K_2/F is an algebraic extension.

We can continue in this way and construct an ascending chain of fields

$F \subset K_1 \subset K_2 \subset \cdots$

such that

1) all fields K_n are finite or countable,
2) $f_n(t)$ has a root in K_n,
3) K_n / F is an algebraic extension.

The union $K = \bigcup_{n \geq 1} K_n$ is a field. The field K is no more than countable.

Every polynomial ~~f_{nn}~~ over F of degree ≥ 1 has a root in K.

The extension K/F is algebraic.

Let $K = K^{(1)}$. Applying the above statement to the field $K^{(1)}$ we get a field

$$K^{(1)} \subset K^{(2)}$$

such that

1) the field $K^{(2)}$ is $\leq$ countable

2) every polynomial from $K^{(1)}$ (of degree ≥ 1) has a root in $K^{(2)}$,

3) the extension $K^{(2)}/K^{(1)}$ is algebraic.

Since both $K^{(2)}/K^{(1)}$ and $K^{(1)}/F$ are algebraic it follows that the extension $K^{(2)}/F$ is algebraic.

And so on. We get an ascending chain of fields

$$F \subset K^{(1)} \subset K^{(2)} \subset K^{(3)} \subset \dots$$

such that every field $K^{(n)}$ is $\leq$ countable, every polynomial from $K^{(n)}$ (of degree ≥ 1) has a root in $K^{(n+1)}$, all extensions $K^{(n)}/F$ are algebraic. Now let

$$L = \bigcup_{n \geq 1} K^{(n)}.$$

The field L is $\leq$ countable; L is algebraically closed; the extension L/F is algebraic.

Let us show that L is algebraically closed. Choose an arbitrary polynomial $f(t) = a_0 + a_1 t + \ldots + a_d t^d \in L[t]$, $d \geq 1$, $a_d \neq 0$.

~~Since L is a union the~~ Let $a_0 \in K^{(n_0)}$, $a_1 \in K^{(n_1)}, \ldots, a_d \in K^{(n_d)}$. Let $n = \max(n_0, n_1, \ldots, n_d)$. Then $a_0, a_1, \ldots, a_d \in K^{(n)}$, $f(t) \in K^{(n)}[t]$. Then $f(t)$ has a root in $K^{(n+1)}$ and, therefore, in L. $\square$